MSTP Pamphlet 6-0.1

# Information Management Guide


MAGTF Staff Training Program (MSTP)

U.S. Marine Corps

October 1998

MSTP Pamphlet 6-0.1

# Information Management Guide

This pamphlet supports the academic curricula of the Marine Air Ground Task Force Staff Training Program (MSTP).

U.S. Marine Corps
October 1998

UNITED STATES MARINE CORPS
MSTP Center (C 467) MCCDC
3300 Russell Road
Quantico, Virginia 22134-5069

5 October 1998

## FOREWORD

1. PURPOSE. MSTP Pamphlet 6-0.1, *Information Management Guide*, is designed to support the operating forces by providing commanders and their staffs with some techniques and procedures required to use information management to support planning, decisionmaking, execution, and assessment.

2. SCOPE. This pamphlet provides guidelines for establishing an organized and disciplined approach for information management. It further provides a methodology to manage relevant, timely information. While the information contained here is scalable to the entire range of Marine air-ground task forces (MAGTFs), the focus of this pamphlet is the Marine expeditionary force (MEF).

3. SUPERSESSION. None.

4. CHANGES. Recommendations for improvements to this pamphlet are encouraged from commands as well as from individuals. The attached User Suggestion Form can be reproduced and forwarded to:

Commanding General (C 467)
Training and Education Command
3300 Russell Road
Quantico, Virginia 22134-5001

Recommendations may also be submitted electronically to:
opso@mstp.quantico.usmc.mil

5. CERTIFICATION. Reviewed and approved this date.

R.K. DOBSON, JR.
Colonel, U.S. Marine Corps
Director
MAGTF Staff Training Program Center
Marine Corps Combat Development Command
Quantico, Virginia

Throughout this pamphlet, masculine nouns and pronouns are used for the sake of simplicity. Except where otherwise noted, these nouns and pronouns apply to either sex.

USER SUGGESTION FORM

From:
To: Commanding General, Marine Corps Combat Development Command (C 54), 3300 Russell Road, Quantico, Virginia 22134-5001

1. In accordance with the Foreword, individuals are encouraged to submit suggestions concerning this Pamphlet directly to the above addressee

Page _____ Article/Paragraph No. _____

Line No. _____ Figure/Table No. _____

Nature of Change: Add Delete
Change Correct

2. Proposed Text: (Verbatim, double-spaced; continue on additional pages as necessary.

3. Justification/Source: (Need not be double-spaced.)

NOTE:
1. Only one recommendation per page.
2. Locally reproduced forms may be used for e-mail submissions to:
opso@mstp.quantico.usmc.mil

This page intentionally left blank.

Record of Changes

| Change No. | Date of Change | Entry Date | Organization | Signature |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

This page intentionally left blank.

## Table of Contents

Part I

# Introduction

MCDP 6 Command and Control says:

> *Information is the words, letters, numbers, images, and symbols we use to represent things, events, ideas, and values. Information is how we give structure and shape to the material world, and it thus allows us to give meaning to and to gain understanding of the events and conditions which surround us.*

## 1001. Information Management

Information management (IM) is defined in *OMB Circular No. A-130 Management of Federal Information Resources* as follows:

> *The term "information management" means the planning, budgeting, manipulating, and controlling of information throughout its life cycle.*

This Circular provides uniform government-wide information resources management policies. It directs the Secretary of Defense to develop:

> *... standards and guidelines to ensure national security, emergency preparedness, and continuity of government.*

The proposed specific definition within Department of Defense for IM is in MCRP 6-23A, *Joint Task Force Information Management*. It states:

> *Information management (IM) refers to the processes a JTF uses to obtain, manipulate, direct and control information. IM includes all processes involved in the creation, collection and control, dissemination, storage and retrieval, protection, and destruction of information.*

Just as we start with a common definition of IM, we must be clear on how the Marine Corps describes the nature of information. MCDP 6, *Command and Control* provides this perspective:

> *Most information grows stale with time, valuable one moment but irrelevant or even misleading the next.*
>
> *There are two basic uses for information. ... to help create situational awareness as the basis for a decision (and) to direct and coordinate actions in the execution of the decision.*
>
> *Given information-gathering capabilities today, there is a distinct danger of overwhelming commanders with more information than they can possibly assimilate. In other words, too much information is as bad as too little-and probably just as likely to occur. The critical thing is not the amount of information, but key elements of information, available when needed and in a useful form, which improves the commander's awareness of the situation and ability to act.*

The goal of IM is providing a timely flow of quality information enabling the commander of a MAGTF to anticipate and understand the consequences of changing conditions. This pamphlet provides the MAGTF headquarters a variety of techniques to manage information efficiently.

## 1002. Information Management and Decisionmaking

Skillful decisionmaking is central to the art of command. Judgment, experience, and vision are some of the factors facilitating skillful decisionmaking. Perhaps the paramount factor is situational awareness. Awareness and understanding of the battlespace allow the MAGTF commander to anticipate future conditions, formulate concepts of operations (CONOPS), analyze courses of action (COAs), and accurately assess risks. In the past, commanders made decisions based on where they understood the threat to be relative to their forces. They depicted on map boards with overlays the information necessary to plan, execute, and assess operations. This graphic depiction of the battlespace, enhanced with text files (e.g., messages, reports, etc.), provided the commander a common tactical picture (CTP). This graphic and text information combined with the commander's experience—intuitive reasoning—enabled him to make sound and timely decisions.

Technology is changing and automating the age-old method of achieving a CTP. Simultaneous distribution of planning information to multiple units is a reality. We display in an automated dynamic manner—instead of traditional map boards—friendly and threat air, ground, surface, and subsurface unit locations and status.

Today, commanders and staff rely on a variety of automated systems to meet information requirements. The advances in communications and computing equipment place an enormous amounts of information virtually at the commander's fingertips. More information is available than humans have the capacity to assimilate, collate, and evaluate. Commanders are becoming victims to system success by losing control of the information they need to support decisionmaking.

Information systems continue to play an important role in building situation awareness. Two principle considerations help to improve the utility of these systems in supporting the decisionmaking process. First, information users at all levels need to change the way they think about information. Instead of thinking of information in terms of systems, think of information as a commodity. Consider information as an input to the decisionmaking process. This assists the staff in focusing on what the commander needs, when he needs it, and presenting it in a usable format to complete the decisionmaking process. Second, the MAGTF must develop a plan for managing information. This ensures that the required information is available in each process leading to required decisions.

## 1003. Information Management Plan

IM requirements vary greatly, and this pamphlet can not cover all of the possibilities. Therefore, MAGTFs must develop an information management plan (IMP) tailored to manage information within the context of their mission and capabilities. An effective IMP provides guidance ensuring the availability of quality information throughout the MAGTF headquarters. The MAGTF commander can then correctly assess changing conditions, establish priorities, and facilitate the decisionmaking process. The MAGTF IMP should cover MAGTF unique IM needs including the duties, responsibilities, and skill requirements; IM systems and requirements, IM processes and procedures; and IM system protection. The

MAGTF IMP should include specific guidance for the management of the MAGTF CTP, collaborative planning systems (CPSs), requests for information (RFIs) management procedures, and network applications used to post MAGTF information. This guidance may also include using news groups, web pages, or other applications.

The development and execution of an effective MAGTF IMP requires the participation and interaction of the commander, chief of staff, all staff sections, and MAGTF elements.

## 1004. Information Quality Characteristics

Quality information adds value to MAGTF staff processes. Information is susceptible to distortion and deception. When developing the IMP, the information management officer (IMO) must consider the following information quality characteristics—

- **Accuracy**. Information that conveys the true situation.
- **Relevance**. Information that applies to the mission, task, or situation at hand.
- **Timeliness**. Information that is available in time to make decisions.
- **Usability**. Information that is in common, easily understood format and displays.
- **Completeness**. All necessary information required by the decisionmaker.
- **Brevity**. Information that has only the level of detail required.
- **Security**. Information that has been afforded adequate protection where required.

## 1005. Information Hierarchy

Reducing uncertainty and increasing the MAGTF commanders situational awareness are the focus of IM processes. IM processes use data and information that have been processed or displayed in a form that is understandable to the people who must use them to enhance situation awareness. See figure 1-1. MCDP 6, *Command and Control*, says:

*We use the term information generically to refer to all manner of descriptions or representations from raw signals on the one hand to knowledge and understanding on the other. But it is important to recognize that there are actually four different classes of information. We must understand the differences between these classes because they are of different value in supporting command and control. We must also understand what happens to information as it moves between levels on the info hierarchy.*

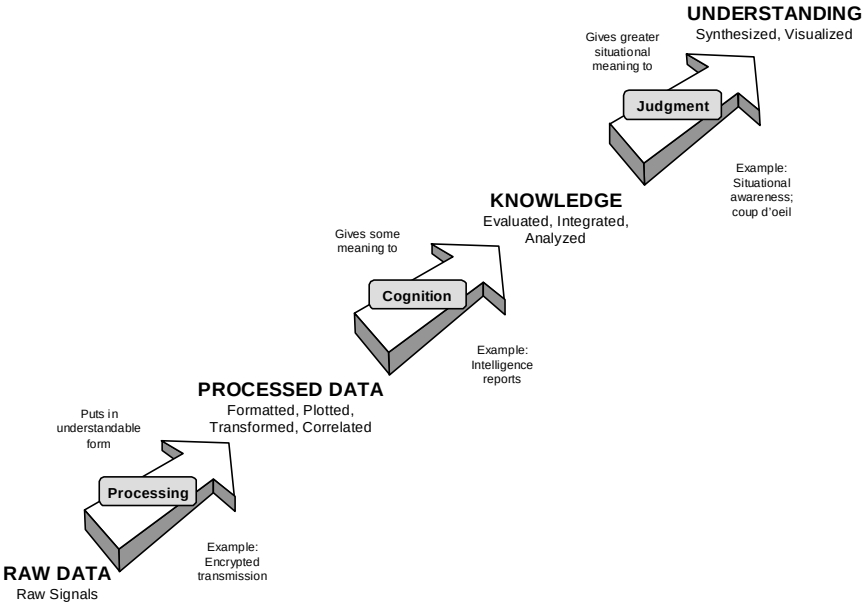


Figure 1-1. Information hierarchy.

## a. Raw Data

Raw data are the lowest class of information and include raw signals picked up by a sensor of any kind (a radio antenna, an eyeball, a radar, a satellite) or sent between any types of nodes in a system. Raw data are signals which have not been processed, correlated, integrated, evaluated, or interpreted in any way. This class of information is rarely of much use until transformed in some way to give it some sort of meaning. Examples of raw data are the bits and bytes transferred between computers or a piece of unprocessed film.

## b. Processed Data

This class of data has been processed into or has been displayed in a form that is understandable to the people who must use them. The act of processing gives the data a limited amount of value. Processed data may have some immediate, obvious and significant value but have not been evaluated or analyzed. Some examples of processed data are film that has been developed into a photograph or grid coordinates plotted on a map.

## c. Knowledge

The next rung on the information hierarchy is knowledge- data that have been analyzed to provide meaning and value. Knowledge is various pieces of processed data that have been integrated and interpreted to begin to build a picture of the situation. At this level we are starting to get a product which can be useful for decisionmaking. For example, military intelligence is a form of knowledge as compared to combat information and situation reports. When pieced together however, they create an estimate of the situation that represents knowledge.

## d. Understanding

The highest class of information is understanding- knowledge that has been synthesized and applied to a specific situation to gain a deeper level of awareness of that situation. Understanding results when we synthesize bodies of knowledge, use judgment and intuition to fill the gaps, and arrive at a complete mental image of the situation. We try to use understanding as a basis for our decisionmaking. Examples are: understanding reveals the enemies critical vulnerabilities; understanding reveals the critical factors in any situation; and understanding allows us to anticipate events.

We should note that as information moves up the hierarchy from data toward understanding, an integration occurs. We piece together multiple bits of raw data to make processed data. Many pieces of processed data coalesce into knowledge. Various elements of knowledge distill into understanding. This integration is essential to achieving understanding. We know that it takes a certain amount of time and effort to make these integrations. But without this effort, a staggering number of things would overload the commander in his decisionmaking. Commanders need knowledge and understanding to make decisions.

The goal of command and control is effective and efficient conduct of military actions. To accomplish this goal, the commander will need information that allows him to attain understanding in a timely manner of a given situation or condition.

An image is the embodiment of our understanding of a given situation or condition. By providing the commander with information in the forms of images, augmented with text descriptions, we put him in a better position to make timely, relevant decisions. A weather report would be one example or a well-conceived, graphically oriented concept of operations and commander's intent should convey a clear and powerful image of the action and the desired outcome.

## 1006. Information Flow

MAGTF IM procedures must provide for the rapid flow, vertical and horizontal, of information. Most MAGTF staff processes require a cross-functional and cross-staff section exchange of information. Traditional staff relationships help determine where information should flow within an organization but these relationships should not form firewalls to the information exchange. Effective flow of information within the various MAGTF processes requires the information to be:

- **Positioned Properly**. The MAGTF need for specific types of information are often predictable. Positioning the required information at its anticipated points of need speeds the flow and reduces demands on communications systems. An example would be using public folders to post required information.
- **Mobile**. The reliable and secure flow of information must be commensurate with the MAGTF's mobility and tempo of operations. Information flow must immediately adjust to support the vertical and lateral flow of information between adjacent forces. An example would be the CPS.
- **Accessible**. All levels of command must be able to pull the information they need to support concurrent or parallel planning and mission execution. If possible, transmit information to the required user via automated means reducing the need for manual exchange. An example of this is the graphic depiction of forces in the CTP.

- **Fused**. We receive information from many sources, in many mediums, and in different formats. Fusion is the logical blending of information from multiple sources into an accurate, concise, and complete summary. An example of this would be the threat assessment disseminated in graphic form on an automated CTP system.

The MAGTF command, control, communications, computer, and information (C4I) systems provide the means for information dissemination. Users of the information are ultimately responsible for its management. Principal and special staff members must clearly identify their information requirements and work closely with the MAGTF IMO ensuring processes are automated in the most effective way possible.

The IMP should include procedures to filter, fuse, prioritize, and disseminate required information. This pamphlet discusses these concepts.

- Filtering is a process of organizing information based on specific criteria.
- Fusion assesses information from multiple sources and develops a concise and complete summary of the situation.
- Prioritization focuses the efforts of the MAGTF headquarters on developing information supporting the commander's decisionmaking process.

Information flow within the MAGTF is a complex yet vital function for reducing uncertainty and ambiguity while facilitating a clear understanding of the battlespace for the commander. Optimum information flow within the MAGTF requires both speed and clarity of transfer without creating fragmented or useless information. The IMP should assign responsibilities and provide instructions on managing information for the MAGTF. This is a vital step ensuring commanders have the required information, when they need it, and in an understandable format.

## Part II

# Duties and Responsibilities

This part identifies the principal managers of MAGTF IM and outlines some of their responsibilities. An organized and disciplined effort is necessary by all personnel to ensure an uninterrupted flow of information. Every user has inherent responsibilities to acquire, assess, reason, question, correlate, and disseminate quality information to other users. All MAGTF personnel, as information users, are also information managers. As information users, each member of the MAGTF must continuously ask the following three questions:

- **Does the information I need already exist?** Valuable time is wasted developing information—point papers, briefings—if the information already exists. Dealing with multiple requests for the same information wastes administrative effort. One solution is developing a CPS that supports information requirements necessary to support planning, decisionmaking, execution, and assessment.
- **Who else needs the information?** Sharing information is essential to maintain unity of effort, and synchronization of operations. Users must consider who—higher, lower, and laterally—requires the information to assist in developing solutions.
- **What is the most efficient and effective way to transfer the information?** Many times the initial reaction to receipt of seemingly important information is to send an e-mail to "All MAGTF Staff". Newsgroups, web sites, and public folders are increasingly popular methods for transferring important information. However, posting information to a newsgroup, homepage, and public folder is no guarantee of receipt by the intended audience. Understanding the process—information flow—that satisfies each critical MAGTF requirement enables all personnel to determine the most efficient and effective means to transfer information. Consideration must be given to whether using newsgroups, web sites, or public folders are timely for critical actions such as transmitting fragmentary orders (FRAGOs) or warning orders. Occasionally,

direct contact is a more appropriate means. Figure 2-1 depicts the matching of some information exchange systems to their intended audience.

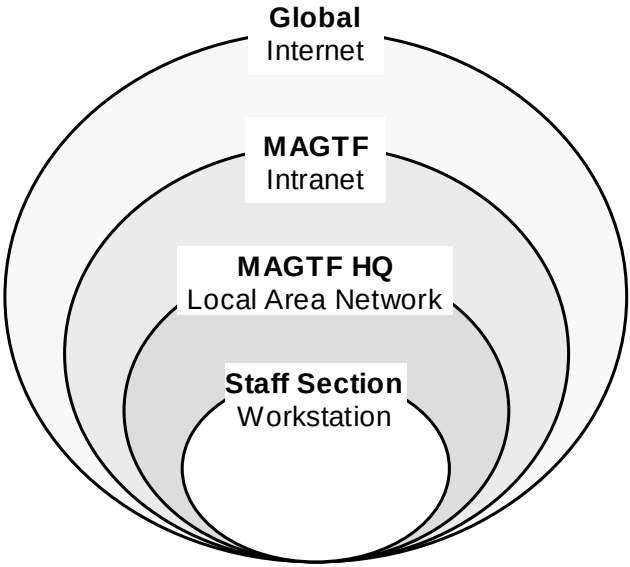


Figure 2-1. Information exchange systems.

A host of other computer-based systems and equipment may be used to exchange information including: radio, telephone, e-mail, Automatic Digital Network (AUTODIN), Defense Message System, video teleconferencing (VTC), etc. The dependency of the MAGTF on automated systems increases the exploitation value of these systems by the enemy.

## 2001. MAGTF Headquarters' Responsibilities

### a. Commander

The commander is responsible to—

- Establish the priorities for information gathering and reporting by establishing the commander's critical information requirements (CCIR), outlined in Part IV.

- Approve the IMP.
- Approve the communications plan that supports the IMP.

### b. Chief of Staff

The chief of staff is responsible to—

- Approve the MAGTF operations cycle.
- Implement the IMP.
- Appoint the MAGTF IMO.
- Appoint a MAGTF web administrator and a MAGTF web grandmaster, if web technology is used.
- Approve format and structure of information posted and distributed from the MAGTF.

### c. Principal Staff Officers

The principal staff officers are responsible to—

- Establish internal staff section procedures for newsgroups, homepages, message handling, e-mail, RFI, and suspense control procedures.
- Appoint a staff section IMO as a point of contact for IM matters.
- If web technology is used, appoint a webmaster for their section.
- Ensure training on basic IM, and security procedures for staff section personnel.
- Assess IM to assure quality and flow and establish benchmarks to evaluate efficiency and effectiveness of IM.

### d. MAGTF G-6

The MAGTF G-6 is responsible to—

- Work closely with the MAGTF IMO to develop the MAGTF communications plan.
- Establish a technical help desk for network and systems administration issues for information systems.
- Establish e-mail accounts.
- Consolidate a list of communications and systems requirements.
- Produce the MAGTF telephone and e-mail directories.

- Establish a central location and procedure for conducting virus scanning of incoming diskettes and laptops.
- Manage networks and network services.
- Ensure system training and familiarization for MAGTF staff and augmentees.

### e. MAGTF Combat Operations Center

The MAGTF combat operations center (COC) is responsible to—

- Assess the information flow to support MAGTF operations, and monitors the efficiency, effectiveness, and accuracy of the MAGTF's CTP.
- Maintain a master suspense action log.
- Maintain a chronological record of significant events.
- Ensure daily briefings and FRAGO production.
- Work closely with the MAGTF intelligence operations center (IOC) to assess, update, and integrate information requirements.

### f. MAGTF Intelligence Operations Center

The MAGTF IOC is responsible to—

- Review, assess, and disseminate required threat information and/or graphic products to support the CTP.
- Monitor the efficiency, effectiveness, and accuracy of the threat assessment displayed by the CTP.
- Work closely with the COC to assess, update, and integrate information requirements.

## 2002. MAGTF Common Tactical Picture Manager

The MAGTF CTP manager is responsible to—

- Develop CTP procedures.
- Operate closely with IMO, COC and IOC watch officers, and principal staff officers.
- Act as focal point for coordinating the CTP within the MAGTF.

## 2003. MAGTF Information Management Officer

The MAGTF IMO is responsible to—

- Develop and publish the IMP.
- Publish the headquarters daily operations cycle.
- Publish the MAGTF report matrix.
- Coordinate additional training requirements for staff members supporting IM.
- Develop effective, efficient track/location management procedures.
- If web technology is used, work closely with the web administrator to establish the web site infrastructure to facilitate the necessary information exchange throughout the MAGTF.

The MAGTF IMO may be an officer or non-commissioned officer regardless of rank or military occupational specialty, as best meets the requirements of the MAGTF. However selection should reflect best use of trained personnel and existing expertise.

## 2004. Staff Section Information Management Officer

The staff section IMO is responsible to—

- Oversee the internal and external information flow of their staff section.
- Provide the MAGTF IMO with staff section information requirements for incorporation into the MAGTF IMP.
- Ensure compliance with the IMP for establishing newsgroups and/or web sites, message handling, e-mail, RFI, and suspense control procedures.
- Coordinate/conduct IM training for staff section members.

The staff section IMO may be an officer or non-commissioned officer regardless of rank or MOS, as best meets the requirements of the staff section. However selection should reflect best use of trained personnel and existing expertise.

## 2005. End User Responsibilities

The end user is responsible to—

- Ensure accuracy of MAGTF information.
- Properly control, classify, protect, and archive all MAGTF information and information systems for which they are responsible.
- Validate the authority to destroy MAGTF information before destruction.
- Read and comply with the information requirements published in the IMP.

## 2006. MAGTF Network Management Responsibilities

If the MAGTF chooses to use web technology, four distinct roles should be identified and their responsibilities established; MAGTF web administrator, MAGTF web grandmaster, webmasters, and information producers.

### a. MAGTF Web Administrator

The web administrator is responsible for the overall management of information on the MAGTF web site. He must coordinate with the various staff sections and elements ensuring establishment of the web site infrastructure facilitating the necessary information exchange throughout the MAGTF. It is not a technical role, although an understanding of web technology is required. The web administrator ensures maintenance of the posted information in accordance with the IMP. The MAGTF IMO may also be designated the web administrator.

### b. MAGTF Web Grandmaster

The grandmaster must work closely with the MAGTF web administrator and the MAGTF IMO for the technical development of the MAGTF web site. The grandmaster coordinates the activities of the webmasters throughout the MAGTF.

### c. Webmaster

By contrast, the webmaster is responsible for the technical infrastructure of the web site to include templates and forms. His primary responsibility is

installing new network management technologies, management, and help their respective elements or staff sections use them. The webmaster provides the tools enabling users to publish, access, and customize information themselves rather than doing it all for them. He should assist in converting documents to appropriate hypertext markup language format, and ensure that hypertext transfer protocols remain current.

### d. Information Producers

Each MAGTF element and staff section, as producers of information, determines what information they create and maintain on the web site. The information producer is responsible for keeping their portion of the MAGTF web site at their level and below current and accurate.

This page intentionally left blank.

## Part III

# Information Management Systems

The goal of information systems and IM procedures is to produce an accurate picture of the battlespace and support decisionmaking, allowing timely mission execution. Information systems must provide effective and secure information exchange throughout the MAGTF. Users need to develop an understanding of the information systems available and create IM procedures to match their information requirements. Below is a brief summary of information systems linked to the warfighting function they support.

By analyzing the information flow required to satisfy each essential warfighting requirement, recommendations can be made as to which C4I systems should be applied to satisfy the required information.

Currently, the Marine Corps uses the following systems to support MAGTF warfighting functions:

- Intelligence Analysis System to support *intelligence*.
- Tactical Combat Operations to support *maneuver*.
- Advanced Field Artillery Tactical Data System to support *fires*.
- Contingency Theater Automated Planning System to support aviation *command and control*.
- MAGTF Tactical Warfare Simulation to support *command and control*.
- Logistics Automated Information System to support *logistics*.
- Global Command and Control System to support *command and control*.
- Command and Control Personal Computer (C2PC) to support *command and control*.
- Microsoft Exchange, Microsoft Office, and Microsoft Outlook to support all warfighting functions in a collaborative environment.

Web pages/newsgroups, e-mail and local area networks are examples of information capabilities that are available today. All information systems exist to support decisionmaking. Having an accurate timely CTP also supports decisionmaking.

## 3001. Common Operational Picture and Common Tactical Picture

The common operational picture (COP) is the integrated capability to receive, correlate and display a CTP, including planning applications and theater-generated overlays/projections (i.e., meteorological and oceanographic (METOC), battle plans, force position projections). Overlays and projections may include location of friendly, hostile and neutral units, assets, and reference points. The COP may include information relevant to the tactical and strategic level of command. The COP serves as a management tool for the combatant commander and his staff. The COP and CTP are not specific depictions of the actual operational or tactical situations. Rather, users apply filters to the COP and CTP to build views of the situation specific to their needs.

CTP is a subset of COP. The CTP is the current depiction of the battlespace for a single operation within a combatant commander's area of responsibility including current, anticipated or projected, and planned disposition of hostile, neutral and friendly forces as they pertain to US and multinational operations. The CTP includes force location, real time and non-real time sensor information, and amplifying information such as METOC. The CTP serves as a command and control tool for the following commanders and their staffs:

- Joint task forces (JTFs).
- Marine Corps components.
- MAGTFs.

Figure 3-1 shows the flow of the COP/CTP with two independent JTFs.

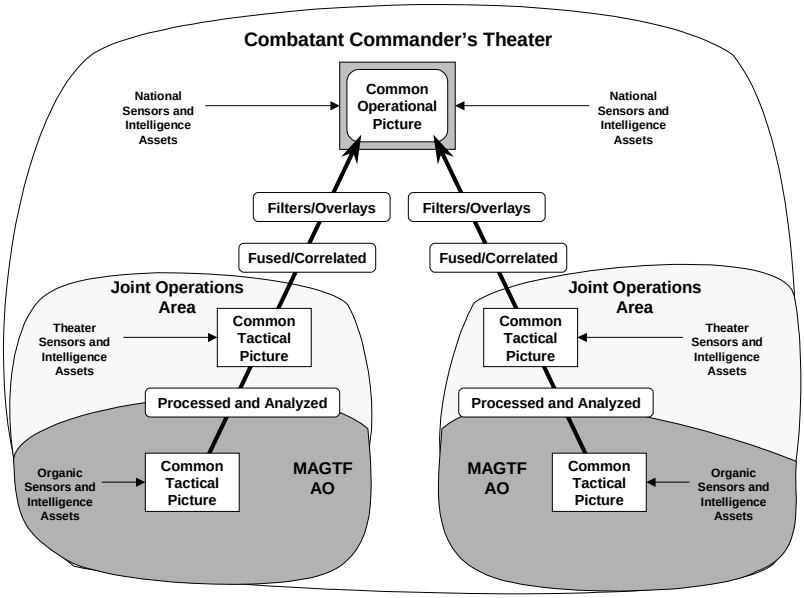


Figure 3-1. Common operational picture/common tactical picture flow.

## 3002. Network Application Management

Networking technologies are expanding the options available for managing the flow of information. We can achieve a collaborative environment for sharing information using web pages, newsgroups, public folders, and e-mail. Networks provide the MAGTF access to unsecure and secure information, allowing users to send and receive unclassified and classified information worldwide. The Unclassified but Sensitive Internet Protocol Router Network (NIPRNET) provides access to the internet. The SECRET Internet Protocol Router Network (SIPRNET) provides access to classified information.

A MAGTF intranet is a communications network where access to information is restricted. The intranet network infrastructure for a MAGTF headquarters may differ from one MAGTF to another, but the concepts are the same. The communication standards of the Internet, and the content standards of the world-wide web are normally the basis for the MAGTF

Intranet. The tools used to create an intranet are normally identical to those used for Internet and Web applications. Using local area networks (LANs) protected by firewalls is normally the method for establishing a MAGTF Intranet structure.

The MAGTF IMO must work closely with the MAGTF Web Administrator, element and staff section IMOs to develop and establish procedures for network management. The MAGTF IMP should identify how the MAGTF headquarters shares critical and relevant information. The MAGTF IMO must establish procedures enabling each staff section to access, post, and update pertinent information. Each staff section ensures the information posted is accurate, current, and relevant.

A well-organized web site assembles vital information, organizes it in a logical sequence, and delivers it efficiently. The MAGTF headquarters, staff sections, and MAGTF elements should develop and maintain their own web pages for the site. Web page information should include, but is not restricted to current updates, status reports, common staff products, and current activities. The MAGTF should organize the web site around a master MAGTF home page. The MAGTF home page—front door—sits at the top of the MAGTF web site acting as a point of entry into the site. Each major element of the MAGTF should have a mini-home page with direct links back to the MAGTF home page.

Users directly access MAGTF site pages via a universal reference locator address. The MAGTF must design the web site so users can quickly navigate regardless of where they enter the site. All MAGTF web pages should include a basic set of links logically connecting them to other web pages on the site.

Newsgroups function like electronic bulletin boards and are a means of disseminating information throughout the MAGTF. The design of the MAGTF newsgroup structure should permit user access to information without burdening them with unneeded information. Newsgroups may be browsed directly or by using the hypertext link structure from a newsgroup home page. The hypertext links have the advantage of leading users directly to the information, without having to browse the entire newsgroup. The newsgroup home page should contain hypertext links to major category newsgroups.

The MAGTF G-6 has the overall responsibility of building, maintaining, and modifying newsgroups in the MAGTF headquarters. The senior communicator at each major subordinate command is responsible for building newsgroups at the their level. The following protocols apply to newsgroup structure and should be reflected in the MAGTF IMP.

- **Newsgroup**. This is the major newsgroup category and is the first hypertext link in the home page newsgroup table.
- **Sub-Group**. Refers to minor categories within the newsgroup. These hypertext links lead the user to the desired information in the newsgroup.
- **Point of Contact**. Refers to the staff section or element responsible for maintaining the newsgroup.
- **Purpose**. A general description of the type of information that may be posted in the newsgroup.

**Caution**. Never assume your intended audience received your information simply because it was posted to a web page or newsgroup. Once information has served its useful lifecycle, remove it from the web page and/or newsgroup.

## 3003. Electronic Mail

Electronic mail (e-mail) can be a highly effective means to communicate information, providing rapid dissemination of time critical information within the MAGTF. It permits a single user to communicate with one or several users simultaneously. E-mail can overload the network is used improperly. Unnecessary information and large message attachments stress the system. Use web sites, newsgroups or public access drives on the LAN to disseminate information. Remove graphics, imagery, and text documents that do not add information content.

## 3004. Video Teleconferencing

Improvements in digital video compression and readily available high-capacity transmission systems make it possible for secure, interactive color video worldwide. The primary purpose of the MAGTF VTC capability is

support of the MAGTF commander. The secondary purpose is to facilitate the transfer of information between subordinate commanders and staffs. Responsibility for scheduling the MAGTF VTC is the chief of staff. The VTC scheduling officer works coordinates with the MAGTF IMO in developing the VTC schedule. Policies and procedures for VTC should reflected in the MAGTF IMP. Because of the range of security classifications potentially passed during a VTC, only personnel with appropriate clearance and access should attend VTCs.

## Part IV

# Requirements, Processes, and Procedures

All commanders depend on information to plan and execute missions. This part focuses on the processes for obtaining and disseminating information within the MAGTF headquarters.

## 4001. Commander's Critical Information Requirements

CCIRs are essentially a prioritized list of critical information requirements verified by the commander as being critical for facilitating decisions or information that is critical for successful mission accomplishment. Using CCIRs focuses the staff on the information the commander requires and has designated as critical. This enhances the staff's ability to filter information and remain focused on the information of the highest value. CCIRs may change as events unfold; decision points pass, or you execute branch plans. Therefore, CCIRs require continuous assessment for relevance to the current and developing situation.

All members of the MAGTF are responsible for reporting information that may satisfy CCIRs. However, each principal staff officer should ensure processes within their staff sections are in place to filter and fuse raw data before submission. CCIR tracking/monitoring is the primary task of the MAGTF COC. When a CCIR is met, or there are indications that one is about to be met, the COC makes an immediate "voice" report to the commander, chief of staff, and principal staff officers. Voice reports are followed by record traffic—flash message, e-mail—to the same distribution list. Once a CCIR is, or is almost answered, the COC analyses the implications of the event on current and developing plans, then briefs the commander.

## 4002. Requests for Information

The MAGTF headquarters establishes the RFI procedures. Joint Publication 1-02 defines the an RFI as:

> *Any specific time-sensitive ad hoc requirement for intelligence information or products to support an ongoing crisis or operation not necessarily related to standing requirements or scheduled intelligence production. A request for information can be initiated to respond to operational requirements and will be validated in accordance with the theater command's procedures.*

RFIs are generated by subordinate, adjacent, and higher headquarters to answer questions that cannot be resolved with organic assets. They are submitted to external agencies *only* if the information does not exist within internal sources. See figure 4-1.

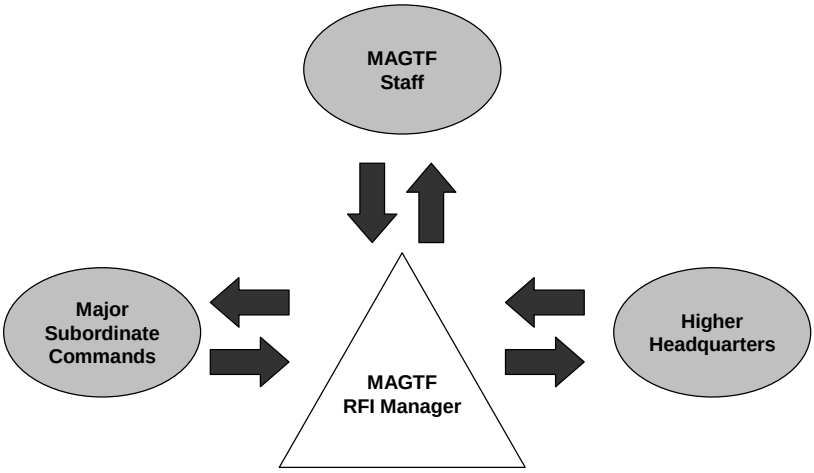


Figure 4-1. Request for information flow.

RFIs pertaining to operations beyond 96 hours in the future should be directed to MAGTF plans, while requests pertaining to operations within the next 24-96 hours should be directed to MAGTF future operations. Information related to current operations should be requested from G-3 current operations in the COC. The G-2 will process intelligence-related

The G-2 will process intelligence-related RFIs, while the G-3 processes all RFIs not specifically related to the gathering and analysis of intelligence. Both staff directorates assign an RFI manager who receives, ensures validation, and prioritizes requests. A tracking system ensures RFIs are processed and information expeditiously disseminated to the requestor.

Staff members submit RFIs electronically as described by the task force RFI management procedures. The RFI managers—G-2 for intelligence RFI, G-3 for all others—validate the request, enter the appropriate information in the tracking system, and update the RFI information page as necessary. When a response is received, the RFI information page is updated and the requester notified.

The following RFI guidelines have proven beneficial to RFI management.

- Limit RFIs to one question per request.
- State RFIs as specific question. Provide sufficient detail so the request in completely understood.
- Spell out acronyms the first time they are used.
- Submit intelligence RFIs through the intelligence RFI system.
- Pass staff section action RFIs to appropriate staff section.
- Format for RFI requests should be approved by the chief of staff and include the following information:
  - Classification.
  - Priority.
  - Time/Date.
  - Required not later than.
  - Requestor.
  - To.
  - Subject.
  - Amplifying data.
  - Recommended method of transmission.
- Intelligence related RFI requests should include the following additional information:
  - Narrative description.
  - Justification.
  - Sources consulted.
  - Date desired.

- Latest time information of value.
- Classification of response.
- Remarks.
- POC.

## 4003. Common Tactical Picture Management

The MAGTF CTP feeds the JTF CTP which in turn feeds the combatant commander's COP. A MAGTF CTP requires effective and efficient management procedures. Some of the data feeds into the CTP are automated, while some are manual. Effective management of the CTP prevents the display of outdated or unwanted surface, air or subsurface locations/tracks in a particular map view.

The MAGTF CTP manager coordinates the actions required to synchronize management between the MAGTF elements and the MAGTF headquarters. The CTP requires the following inputs:

- Blue air, maritime and ground force tracks/locations.
- Red air, maritime and ground force tracks/locations.
- White/neutral/unknown air, maritime and ground force tracks/locations.
- Operational overlays.
- Intelligence overlays.
- National Imaging and Mapping Agency products.

The CPS is a compilation of systems, software applications, and tools designed to support MAGTF planning, decisionmaking, execution, and assessment. The MAGTF CPS should allow input by multiple personnel, both at the MAGTF and at remote locations. The MAGTF CPS should:

- Include an interactive visual projection capability so members of the MAGTF can see the collaborative effort both on their workstation and on a large screen display.
- Support the MAGTF planning process in a series of logical steps and provide an explanation or "how to" section.
- Provide products in the correct format so that a commander's briefing is presented right off the working screens.

- Be capable of scanning documents into required databases so all MAGTF elements can view higher, adjacent, and supporting command orders and messages.
- Include databases which can be accessed to include intelligence feeds, world-wide map system, unit capabilities, equipment, and organization of forces as required.
- Possess the ability to alert and recognize information tethered to CCIRs.
- Possess the capability to print information and overlays contained in the system.
- Possess the capability to portray maps with operational graphics, e.g., boundaries, fire support coordination measures, decision support templates, fire support plans, and barrier plans, etc.
- Have the capability to transfer information from working/briefing formats to a message format to generate messages without having to start from scratch.

Through the use of Microsoft Exchange, Microsoft Office, and C2PC software, a CPS can be developed that allows text, imagery, and graphic information to be shared.

Table 4-1 contains some sample reports, requests, and orders for which the MAGTF may be responsible. The table provides a brief description of the report, the sender, receiver, when and how to transmit, and whether it is in United States Message Text Format.

| Report Title | Submit By | Submit as of | Arrive NLT | Trans Type | Prece dence | Address | Info to |
|---|---|---|---|---|---|---|---|
| Spot Report | All | As Reqr | As Reqr | E-Mail | Routine | G-2 | |
| SITREP | All | 2400Z | 0200Z | AUTODIN/ Home page | Priority | CO/ G-3 | Elements |
| OPORD/ FRAGO | G-3 | As Reqr | As Reqr | AUTODIN/ Home page | Priority | All | Elements |
| RFI (except intel) | All | As Reqr | As Reqr | E-Mail | Priority | RFI Manager | |

Table 4-1. Sample reports.

This page intentionally left blank.

## Part V

# Information and Information Systems Protection

Networks and information systems are high value targets to the enemy and must be adequately protected and defended to maintain the integrity of the MAGTF command and control infrastructure. Increasing reliance on automated information systems for IM will be a MAGTF's "Achilles Heel" if taken advantage of by an adversary. Mission accomplishment depends on protecting and defending information and information systems from destruction, disruption, corruption, and safeguarding these systems from intrusion and exploitation. All Marines must assume their information and information system is a target. All Marines share responsibility for adequately protecting and defending friendly information and information systems. Protection and defense of information and information systems is accomplished through aggressive application of information assurance measures. The primary means to apply information assurance is through information security (INFOSEC), this could include intrusion detection, effect isolation, and incident reaction to restore information and system security. The dynamic nature of the developing information environment requires well-developed information assurance programs to ensure effective IM.

## 5001. Threats to Information Management

Internal and external threats to IM must be anticipated as a part of the IM plan. The various types of threats include:

- Hackers (inside or outside the MAGTF) with limited support and motives to organized and financially backed countries or groups.
- Disgruntled system users.
- Poor communications security, computer security, and operations security practices.
- Viruses (malicious code).

- Unauthorized/Unintentional Disclosure of Data. This threat increases proportionally to the MAGTF's use of automation.
- Corruption of Data. This is an insidious method of deception that, if undetected, leads to faulty guidance, coordination, decisionmaking, and execution.
- Physical Disruption or Denial of Communications. This threat can be internally or externally generated.
- Terrorist groups.
- State sponsored IW attacks.

## 5002. Threat Techniques and Tools

Threats may be easily identified and detected, but difficult to counter. Others may be in place but not activated or detectable. Unusual occurrences during operations should be brought to the attention of the individuals responsible for defense of information and information systems. Examples of threat techniques include:

- Masquerading, or attempting to gain access by posing as an authorized user. Password selection, use, and protection are vital to counter these intrusions.
- Spoofing, or the insertion of data causing a system to inadvertently disclose information or data.
- Electronic warfare can cause denial of service and corruption of data by employing electromagnetic energy. Electromagnetic pulses can corrupt and destroy data stored on magnetic media and damage software and hardware.
- Signals intelligence can provide information in support of other threats. It can provide insight into communications infrastructure and information transfer techniques.
- Substitution and modification disrupts planning and operations by modifying or substituting false data or information in a system. The objective can be to influence a specific plan or operation, and shake the user's faith in the integrity of his information.
- Physical attacks, or destruction because of natural disaster can be a threat to information systems. Facilities and physical resources may be lost, and the loss of connectivity can be devastating.

- Unauthorized access to information processing and transfer resources presumes the threat is internal. Typically, knowledge of an organization's systems, procedures, and security barriers is required.

## 5003. Defensive Information Operations

Defensive information operations (a subset of information operations) are actions to protect and defend one's own information and information systems. MAGTF personnel form an essential line of defense in the way they use today's office automation and networks. Defensive information operations integrate and coordinate policies and procedures, operations, personnel, and technology to protect and defend information and defend information systems. They include:

- Determining the indicators adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information.
- Selecting and executing measures to eliminate or reduce the vulnerabilities of friendly actions to adversary exploitation.
- Identifying critical information resources, then taking all possible measures to deny unauthorized persons information of value that might be derived from intercept and analysis of compromising emanations from cryptographic equipment and telecommunications systems.
- Installation and proper use of cryptographic systems.
- All physical measures necessary to safeguard classified equipment, material, and documents from access or observation thereof by unauthorized persons.
- All measures designed to protect transmissions from interception and exploitation by means other than cryptographic analysis.
- A capability to protect information at rest, being processed, and transitioning terminal devices, switches, networks, and control systems from intrusion, damage, and exploitation.
- Consent to monitoring warning banners.
- Using password protected screen savers.
- Safeguarding passwords. All passwords have to be:
  - Alphanumeric with a minimum of eight characters.
  - Changed regularly.

- Configuration control.
- Information Storage.

Classified data may be stored on floppy disks or tapes that can be secured when not in use or on secure network drives. Classified data may not be stored on the fixed hard drive unless the workstation is located in a certified and approved area.

Removable data storage media will be labeled with the appropriate classification. Examples are the SF 710 (1-87) UNCLASSIFIED Sticker (Green) and the SF 707 (1-87) SECRET Sticker (Red). Removable data media regardless of classification are classified at the highest level authorized for that computer system and marked appropriately.

All floppy diskettes must have an appropriate security label. Mark all magnetic media with the highest level of classification, even if it has been deleted or erased.

The security rules followed for “working paper” copies are followed for floppy disks. If the paper working copy requires an accounting and control number, then the diskette will too. The G-6 INFOSEC staff has information on accounting and control of all diskettes. Be sure to perform routine inventories on all disks, tapes, and CD-ROMs.

All classified magnetic media and CD ROMs being transferred from the MAGTF to another command must go through proper classified mailing and/or courier handling. Procedures must be developed that guide individuals through the proper method of releasing classified information.

Reuse of a disk or tape must be done at the same classification level or higher. If the disk or tape must be used at a lower classification level, approved methods for clearing, overwriting, or purging data from storage media must be used first.

Viruses (malicious code) can be introduced from outside or within the organization. **Viruses in attachments are not currently intercepted by server-based anti-virus software**. Only after an attachment has been "saved as" (decrypted) can virus scanning take place. Viruses in the MAGTF environment reside in three tiers: server, networked workstations,

and diskettes. All members of the MAGTF should use available anti-virus software and comply with the following procedures:

- **MAGTF Server**. At this level, the server's networked, shared drive is scanned for viruses on an automatic basis. The server level is handled by the network system administrator and is transparent to the user. The MAGTF server runs the anti-virus software periodically to catch any infected files placed on the shared drive. The MAGTF G-6 is responsible for server protection.
- **MAGTF Desktop Workstation**. At this level, the user accomplishes virus detection and elimination by initiating virus detection software.
- **Diskettes**. Diskettes act as hosts for the virus to travel from machine to machine. Unless you know otherwise, assume diskettes are infected. Always scan diskettes before use. The MAGTF G-6 will establish a site for conducting virus scanning of incoming diskettes. MAGTF personnel will not be permitted to use diskettes which have not been virus-checked by the G-6. The G-6 will install anti-virus software on the LAN in order for users to check files downloaded from news groups or e-mail. Many liaison officers will bring their own laptop computers to the MAGTF. The G-6 should develop procedures for scanning laptop computers before their use in the MAGTF.

In general, individuals can check for viruses on their workstation by turning their workstations off and on at each shift change if up-to-date anti-virus software is loaded. Procedures should be written and used that direct users to scan all and attachments after saving. The procedures should outline what the individual should do if they discover a virus on their workstation.

## 5004. Unclassified Internet Procedures

When using the internet, observe the following guidelines:

- Do not process or exchange classified information via the internet!
- Internet access is granted for official use only.
- All software downloaded from the internet should be promptly scanned with updated virus detection software.

## 5005. Internet Access

The MAGTF should not restrict the use of the Internet for users with a valid mission need. However, world-wide web pages should NOT be posted on any MAGTF system without approval of G-6 INFOSEC staff. Be aware that information exchanged via the Internet is not necessarily protected and is subject to compromise.

## 5006. Information Destruction

Electronic records should be treated the same as paper records regarding destruction. Dispose of documents that are no longer required. Do this in accordance with the provisions of the Federal Records Act (44 U.S. Code 21 and 33) which specifies disposal instructions. Continue to protect materials identified for destruction—as appropriate for their classification—until then.

Destroy classified documents and material in a way that eliminates risk of reconstruction of the classified information they contain.

- Place burn bags throughout the MAGTF work space, particularly in areas that include printers and copiers. If in doubt, dispose of unneeded classified materials in a burn bag. Control burn bags to minimize the possibility of unauthorized removal of the bag or the contents before destruction. When filled, seal the burn bags in a manner that facilitates detection of any tampering with the bag. Mark sealed bags with an office symbol and the highest classification of the information contained. Keep all required records of destruction.
- Special security handling procedures for clearing and / or purging, destroying, and removal of external markings from magnetic media and CD-ROMs are needed to prevent the unintentional disclosure of information. This includes data remnants, or traces of information remaining on storage media even after the use of purging procedures. Classified storage media should be destroyed when no longer usable.

## Part VI

# Summary

The proposed specific definition within Department of Defense for IM is in MCRP 6-23A, *Joint Task Force Information Management.* It states the following:

> *The processes by which information is obtained, manipulated, directed and controlled. IM includes all processes involved in the creation, collection and control, dissemination, storage and retrieval, protection, and destruction of information.*

The goal of IM is to provide the quality and flow of information which enables the commander to react to changing battlespace conditions, evaluate changing priorities, and dominate the decision cycle. Skillful decisionmaking is central to the art of command. Judgment, experience, and vision are some of the factors facilitating skillful decisionmaking. Perhaps the paramount factor is situation awareness. Awareness and understanding of the battlespace allow the MAGTF commander to anticipate future conditions, formulate CONOPS, analyze COAs, and accurately assess risks.

MAGTFs must develop an IMP tailored to manage information within the context of their mission and capabilities. The MAGTF IMP should cover MAGTF unique IM needs including the duties, responsibilities, and skill requirements; IM systems and requirements, IM processes and procedures; and IM system protection. The MAGTF IMP should include specific guidance for the management of the MAGTF CTP, CPSs, RFI management procedures, and network applications used to post MAGTF information.

MAGTF IM procedures must provide for the rapid flow, vertical and horizontal, of information. The MAGTF C4I systems provide the means for information dissemination. As information users, each member of the MAGTF must continuously ask the following three questions:

- Does the information I need already exist?
- Who else needs the information?

- What is the most efficient and effective way to transfer the information?

The goal of information systems and IM procedures is to produce an accurate picture of the battlespace and support decisionmaking, allowing timely mission execution. Information systems must provide effective and secure information exchange throughout the MAGTF.

The COP is the integrated capability to receive, correlate and display a CTP, including planning applications and theater-generated overlays/projections (i.e., METOC, battle plans, force position projections). The COP serves as a management tool for the combatant commander and his staff.

CTP is a subset of COP. The CTP refers to the current depiction of the battlespace for a single operation within a combatant commander's area of responsibility including current, anticipated or projected, and planned disposition of hostile, neutral and friendly forces as they pertain to US and multinational operations. The CTP includes force location, real time and non-real time sensor information, and amplifying information such as METOC. The CTP serves as a command and control tool for the following commanders and their staffs:

- JTFs.
- Marine Corps components.
- MAGTFs.

We can achieve a collaborative environment for sharing information using web pages, newsgroups, public folders, and e-mail. The communication standards of the Internet, and the content standards of the world-wide web are normally the basis for the MAGTF intranet. Newsgroups function like electronic bulletin boards and are a means of disseminating information throughout the MAGTF. The MAGTF G-6 has the overall responsibility of building, maintaining, and modifying newsgroups in the MAGTF headquarters.

E-mail can be a highly effective means to communicate information, providing rapid dissemination of time critical information within the MAGTF. It permits a single user to communicate with one or several users simultaneously.

The primary purpose of the MAGTF VTC capability is support of the MAGTF commander. The secondary purpose is to facilitate the transfer of information between subordinate commanders and staffs.

CCIRs are essentially a prioritized list of critical information requirements verified by the commander as being critical for facilitating decisions or information that is critical for successful mission accomplishment. Using CCIRs focuses the staff on the information the commander requires and has designated as critical.

RFIs are generated by subordinate, adjacent, and higher headquarters to answer questions that cannot be resolved with organic assets. RFIs are submitted to external agencies *only* if the information does not exist within internal sources.

The CPS is a compilation of systems, software applications, and tools designed to support MAGTF planning, decisionmaking, execution, and assessment. The MAGTF CPS should allow input by multiple personnel, both at the MAGTF and at remote locations. Through the use of Microsoft Exchange, Microsoft Office, and C2PC software, a collaborative planning system can be developed that allows text, imagery, and graphic information to be shared.

Networks and information systems are high value targets to the enemy and must be adequately protected and defended to maintain the integrity of the MAGTF command and control infrastructure. Internal and external threats to IM must be anticipated as a part of the IM plan. Defensive information operations (a subset of Information Operations) are actions to protect and defend one's own information and information systems.

Viruses (malicious code) can be introduced from outside or within the organization. **Viruses in attachments are not currently intercepted by server-based anti-virus software**. Diskettes act as hosts for the virus to travel from machine to machine. Unless you know otherwise, **assume diskettes are infected**. Always scan diskettes before use.

This page intentionally left blank.

## Appendix A

# Glossary

### Section I
### Acronyms

**Note:** Acronyms change over time in response to new operational concepts, capabilities, doctrinal changes and other similar developments. The following publications are the sole authoritative sources for official military acronyms:

1. Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*.
2. MCRP 5-12C, *Marine Corps Supplement to the Department of Defense Dictionary of Military and Associated Terms*.

| | |
|---|---|
| AUTODIN | Automatic Digital Network |
| C2PC | Command and Control Personal Computer |
| C4I | command, control, communications, computers, and intelligence |
| CCIR | commander's critical information requirement |
| COA | course of action |
| COC | combat operations center |
| COP | common operational picture |
| CONOPS | concept of operations |
| CPS | collaborative planning system |
| CTP | common tactical picture |
| FRAGO | fragmentary order |
| IM | information management |
| IMO | information management officer |
| IMP | information management plan |

| | |
|---|---|
| INFOSEC | information security |
| IOC | intelligence operations center |
| JTF | joint task force |
| LAN | local area network |
| MAGTF | Marine air-ground task force |
| MEF | Marine expeditionary force |
| METOC | meteorological and oceanographic |
| MSTP | MAGTF Staff Training Program |
| NIPRNET | Unclassified but Sensitive Internet Protocol Router Network |
| RFI | request for information |
| SIPRNET | SECRET Internet Protocol Router Network |
| VTC | video teleconference |

## Section II
## Definitions

**Note:** Definitions of military terms change over time in response to new operational concepts, capabilities, doctrinal changes and other similar developments. The following publications are the sole authoritative sources for official military definitions of military terms:

1. Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*.
2. MCRP 5-12C, *Marine Corps Supplement to the Department of Defense Dictionary of Military and Associated Terms*.

---

### C

**commander's critical information requirements**—A comprehensive list of information requirements identified by the commander as being critical in facilitating timely information management and the decision making process that affect successful mission accomplishment. The two key subcomponents are critical friendly force information and priority intelligence requirements. Also called **CCIR**. (JP 1-02)

### C

**Command and Control Personal Computer**—C2PC is a Windows-based software application designed to facilitate military command and control functions. Used as a stand-alone tool, trained C2PC operators can produce digital overlays and operational graphics for a unit's internal use. When connected to a C4I computer network, complete with a tactical database manager, C2PC has the capability of visually depicting the locations of friendly and enemy units, as well as to transmit doctrinal overlays. (MSTP Pamphlet 6-5)

### D

**defensive information operations**—The integration and coordination of policies and procedures, operations, personnel, and technology to protect

and defend information and information systems. Defensive information operations are conducted through information assurance, physical security, operations security, counter-deception, counter-psychological operations, counterintelligence, electronic warfare, and special information operations. Defensive information operations ensure timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and information systems for their own purposes. (JP 1-02)

## I

**information management**—The processes by which information is obtained, manipulated, directed, and controlled. IM includes all processes involved in the creation, collection and control, dissemination, storage and retrieval, protection, and destruction of information. (MCPR 6-23A.)

**information security**—Information security is the protection of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users. Information security includes those measures necessary to detect, document, and counter such threats. Information security is composed of computer security and communications security. Also called **INFOSEC**. (JP 1-02)

## W

**webmaster**—The person who administers a website. The webmaster is often also the designer of some or all of the site's pages.

**web pages**—Web pages are documents on the Internet or an intranet. A Web page consists of an HTML file, with associated files for graphics, scripts, and controls, in a particular directory on a particular computer.